STRATEGY
RESEARCH
PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

THE LEGAL AND ETHICAL IMPLICATIONS OF INFORMATION OPERATIONS

BY

MR. OLLIE WASHINGTON, JR.
Department of the Army Civilian

DISTRIBUTION STATEMENT A:
Approved for Public Release.
Distribution is Unlimited.

USAWC CLASS OF 2001

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

THE LEGAL AND ETHICAL IMPLICATIONS OF INFORMATION OPERATIONS

by

Ollie Washington, Jr.
DA Civilian

COL Tom Dempsey
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Ollie Washington, Jr.

TITLE: The Legal and Ethical Implications of Information Operations

FORMAT: Strategy Research Project

DATE: 10 April 2001 PAGES: 22 CLASSIFICATION: Unclassified

Information Operations (IO) is a family of programs and tools that are used to deprive or disrupt an adversary's information and information systems while assuring the continued availability of your own. The technological tools of IO have been developed and implemented so rapidly that the domestic and international laws that should govern their use have not kept pace. Hackers, cyber criminals, terrorist and foreign spies are using tools such as computer network attack while domestic and international laws are insufficient to adequately patrol them. Further, there are ethical issues involved in the use of these IO tools that may not have been adequately debated, at least from a societal standpoint, to mediate possible conflicts with our national values. IO tools will allow the U.S. to engage and disable enemy facilities previously engaged with kinetic weapons, without the physical collateral damage, but with possible significant impact on noncombatants. International agreements such as the Geneva Convention do not specifically address IO and even within the U.S. military the rules of engagement on IO are not clear. This paper will attempt to explore some of these incongruities and provide a perspective on where the U.S. stance could be on our use of IO.

TABLE OF CONTENTS

PREFACE

I would like to thank Colonel Ralph Ghent, Colonel Tom Dempsey and Lieutenant Colonel Nathaniel Perkins for their advice, assistance and guidance in helping me to complete this project.

THE LEGAL AND ETHICAL IMPLICATIONS OF INFORMATION OPERATIONS

Information Operations (IO) is a family of programs and tools that are used by the U.S. military to deprive or disrupt an adversary's information and information systems while assuring the continued availability of its own. The technological tools of IO have been developed and implemented so rapidly that the domestic and international laws that should or could govern their use have not kept pace. Recreational hackers, cyber criminals, terrorists and foreign spies are using tools such as computer network attack while domestic and international laws are insufficient to adequately patrol them. Further, there are ethical issues involved in the use of these IO tools that may not have been adequately debated, at least from a societal standpoint, to mediate possible conflicts with our national values. International agreements such as the Geneva Convention do not specifically address IO and even within the U.S. military, the rules of engagement on IO are not clear. In this paper, I will attempt to explore some of these incongruities and provide my perspective on where the U.S. stance could be on our use of IO. I will provide background information and information systems and the critical role that they play in our society today. I will discuss the components of the IO program and them discuss some of the legal and ethical implications and complications of employing. Finally, I will conclude with my perspectives on how the U.S. can effectively employ IO while remaining consistent with its laws and moral and ethical values.

BACKGROUND.

As advances have been made in the communications, electronics and computer industries, these new technologies have been incorporated into the government, military and civilian sectors of American society. This incorporation has been so complete that these technologies are deeply embedded into the tools that we use every day and whose services we take for granted. Computers and automated processes have enabled us to improve our efficiency, accuracy and productivity while decreasing the manpower required for the same output.

In a similar fashion, the military has developed weapons systems, command and control systems and communications systems that make significant use of high technology systems. Laser rangefinders and targeting systems, global positioning systems, vision enhancement systems and digital switching systems are but a few examples of the applications that the military makes of high technology systems. High technology components are so widely employed in military systems that the divisions of labor between functional areas have become blurred. For instance, the capabilities and user-friendliness of Army communications systems have advanced so far that the line between the combat arms "user" and the communications "provider" is difficult to distinguish. This distinction only becomes clearer as repair and maintainer tasks are needed. The Internet, along with the military Non-classified Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET), has created the ability to distribute information (data, video, and graphics) globally in a near instantaneous manner.

With the increased capabilities provided by high technology systems comes the recognition of a developed dependence on these systems and the assumption of an associated operational vulnerability. In a 1996 report, the Government Accounting Office (GAO) stated:

> The need to protect sensitive and critical federal data has been recognized for years in various laws, including the Privacy Act of 1974; the Paperwork Reduction Act of 1980, as amended; and the Computer Security Act of 1987. However, information security has taken on new significance as both reliance on computers and vulnerabilities associated with networked systems have increased.[1]

The J6 of the Joints Chiefs of Staff further stated:

> Because these information systems are now so important, they have become lucrative targets for numerous threats that we must deter and defeat. We conduct Information Operations (IO) actions to affect adversary information and information systems while defending our own information and information systems that are vital to achieving Information Superiority. Information Assurance (IA) is that part of IO that protects and defends against adversary actions.[2]

As a result of assembling computers, peripheral devices and networks for functional purposes, the U.S. has created a new resource – the National Information Infrastructure (NII).[3] The NII is vital to the national defense and critical government and business services. It is therefore a critical national asset that must be protected. On July 15, 1996, President Clinton issued Executive Order 13010, "Critical Infrastructure Protection." This order established the operation of "The President's Commission on Critical Infrastructure Protection" (PCCIP).

> The Commission, chaired by aerospace industry leader Robert "Tom" Marsh, included senior representatives from private industry, government and academia. An Advisory Committee consisting of industry leaders provided counsel to the Commission and a Steering Committee, made up of cabinet-level officials, reviewed the Commission's report before forwarding it to the President.[4]

On May 22, 1998, President Clinton issued "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63" (PDD 63). This directive absorbed the assessments of the Commission's report and further issued guidance on corrective and preventive actions to be taken within the agencies of the federal government. Some of the key parameters of this directive were[5]:

1. The organization of the federal government agencies (including the appointment of a National Coordinator, a Critical Infrastructure Coordinating Group and a Chief Infrastructure Assurance Officer within each agency) to specifically address infrastructure protection and to conduct interagency coordination on these issues.
2. A 180-day deadline for each department and agency to develop a plan for protecting its own critical infrastructure including, but not limited to, its cyber-based systems.
3. The establishment of a national center to warn and respond to infrastructure attacks.
4. The presentation of the federal government as a model for the rest of the country in addressing infrastructure protection.

As a result of PDD 63, the Federal Bureau of Investigation (FBI) established the National Infrastructure Protection Center (NIPC) with primary responsibility for coordinating national efforts to respond to cyber-crime. In addition to fighting cyber-crime, the FBI was designated the lead agency for coordinating other NII protective measures among other government agencies and civilian entities such as state and municipal governments and U.S. industries.

In the 1999 National Security Strategy, President Clinton cited "Critical Infrastructure Protection" as a major area of threat and directed that a plan for defending critical infrastructures be developed by May 2001 and operational by December 2003.[6] To provide infrastructure protection guidance to the agencies of the Department of Defense, Secretary Cohen, on 10 March 1999, issued "Information Operations Condition (INFOCON)". Administered through the Joint Staff J-3 Directorate of Operations, "The INFOCON system presents a structured, coordinated approach to defend against and react to adversarial attacks on DOD computer and telecommunication networks and systems."[7] This memorandum established policies, procedures and organizational changes to allow the DOD to respond to this new threat.

INFORMATION OPERATIONS.

Information Operations (IO) involves actions taken to effect adversary information and information systems while defending one's own information and information systems.[8] In accomplishing its objectives, IO use five main capabilities or elements: 1) Operational Security (OPSEC), 2) Psychological Operations (PSYOPS), 3) Electronic Warfare (EW), 4) Military Deception and 5) Physical Destruction.[9] These elements are used in both Offensive IO and

Defensive IO. Offensive IO involve the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision makers and achieve or promote specific objectives.[10] Defensive IO integrates and coordinates policies and procedures, operations, personnel and technology to protect and defend information and information systems.[11]

During Offensive IO, OPSEC, PSYOPS and military deception are referred to as perception management actions.[12] These elements are applied towards an enemy and his populace to reduce the amount of information the enemy has about our real plans, while influencing his perception and causing him to respond in a desired manner. Safeguarding classified or sensitive information, distributing leaflets pronouncing the futility of their war efforts and a feint maneuver to conceal the real landing location for an amphibious operation are all examples of perception management operations. EW, composed of electronic attack, electronic protection and electronic warfare support,[13] and physical destruction of an enemy's information and information systems would be employed to degrade or eliminate those capabilities. Computer network attack and system penetrations are Offensive IO actions that would be applied toward enemy computers, computer networks and automated controllers of other essential systems such as air defense systems.

During Defensive IO, the focus would be on protecting friendly information and information systems. The elements of OPSEC, PSYOPS and military deception could still be used to achieve enemy perception management. In Defensive IO, however, the attack element of EW and the physical destruction of enemy systems would not be employed. Other Defensive IO actions would involve computer network defense, network monitoring (for intrusion attempts) and counterintelligence activities. Intelligence gathering and network and system monitoring are some of the contentions areas that will be discussed further in the legal and ethical sections of this paper.

Information Operations within the U.S. military are the responsibility of the Secretary of Defense. The Chairman of the Joint Chiefs of Staff serves as the principal advisor to the Secretary on all IO matters. Within the Joint Staff, the J3, Operations, is responsible for IO. This is accomplished through the J39, Deputy Director for Information Operations.[14] At the Joint Task Force level, IO activities are conducted as directed by the Joint Task Force Commander under the direction of the J3 as the staff element with primary responsibility for IO. [15] The J3 designates an IO Officer who coordinates the operation of the Joint IO Cell.[16] The Joint IO Cell contains representatives from a wide range of activities including the Joint Staff elements (J2 through J7), the Staff Judge Advocate (SJA), Civil Affairs and elements from other supporting activities such as the Joint Special Operations Task Force and the Joint PSYOPS Task Force.[17]

IO is another tool that the military commander has to support him in the execution of his mission. This would appear to be fairly straightforward until we consider the amount of overlap that we now have between what would have formerly been considered a military target and those that now fall into the range of "dual-use systems." This issue is further complicated when we consider such questions as, "Is an enemy command and control center a viable target when it is also the head of the civil government?" When we consider that 90% of the Department of Defense 's (DOD) daily communications travel over civilian owned and operated communications systems,[18] we can see how the distinction between military and civilian "target" has been further clouded.

LEGAL AND ETHICAL IMPLICATIONS.

As high technology systems, especially computer-based systems, have emerged, they have become embedded into production, control and information management functions worldwide. Many systems, such as utilities (e.g., water and electricity), provide services to civilian industries, municipalities and homes as well as military installations. Adversarial nation states must now deal with legal and ethical issues involved in destroying enemy facilities for military purposes. In establishing distinction between military and civilian "targets", technology has created a greater overlap in dual-use facilities that has not been accounted for in the rules of war such as the 1949 Geneva Convention. Globally, there is a tangle of differing capabilities, differing values, differing political systems and a host of differing perceptions of right and wrong and good and evil. Within that context, the U.S., as the lone remaining hegemon, is left to struggle with issues of legalities, ethics, sovereignty and self-defense in employing all of the weapons at its disposal, especially IO. In conducting Offensive and Defensive IO programs, the U.S. must grapple with these issues within the context of peacetime and wartime frameworks.

In beginning a discussion of these issues, it would appear that it would be easier to start with a discussion of IO during a wartime scenario. During wartime, the U.S. could bring all of its conventional resources to bear on the enemy's ability to conduct war and on its civilian populace's will to support that war. Any restrictions that the U.S. would apply to its resources such as IO would be drawn from its moral and ethical value system. Having entered into hostilities, adversaries are limited only by their capabilities and are bound only by internationally drawn rules for the just conduct of war (Jus In Bello) such as the 1949 Geneva Convention.

These rules cover such things as not bombing hospitals, schools and other clearly noncombatant structures. An ethical issue would arise when an enemy decides to cover a military target with human noncombatant shields, such as Saddam Hussein did during the Gulf War. The U.S. was left to decide whether to forego the target or to destroy it because of its military significance and deal with the potential social backlash of killing noncombatants. This latter option would fall under the principle of More Good Than Harm, under the just war fighting tenets.19 The tenets of Just War include Right Purpose, Duly Constituted Authority, Last Resort, Noncombatant Immunity, Proportionality, and More Good Than Harm.

IO can provide an ethical alternative to physical destruction. Rather than destroying an enemy power station, computer attack could be used to render it inoperative. This would accomplish the military objective of turning the power off, while leaving the facility available to be restored after the end of hostilities. Using this IO option could further serve a psychological purpose of convincing the enemy populace that our objective is to end the hostilities and not to destroy their country. While the U.S. would argue that this thought follows deliberate and logical reasoning and would appear far more ethical, there are those that would argue to the contrary.

Because noncombatants are deprived of power in either of the above situations, the argument is being made that the attacker would be guilty of collateral damage. In an article on IO, William Church of the Centre for Infrastructure Warfare Studies, states that IO violates Protocol I Additional to the 4th Geneva Convention of 1949.[20] Mr. Church first substantiates his argument by referring to United Nations Resolution 3384-10 November 1975-which proclaims:

> All states shall refrain from any acts involving the use of scientific and technological achievement for the purpose of violating the sovereignty and territorial integrity of other states, interfering in their internal affairs, waging aggressive wars suppressing national liberation...[21]

Specifically addressing the use of IO against targets such as power plants, Mr. Church invokes Article 54 of Protocol I—Protection of Objects Indispensable to the Survival of the Civilian Population:

> (2) It is prohibited to attack, destroy, remove or render useless objects indispensable to the survival of the civilian population, such as foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies and irrigation works, for the specific purpose of denying them for the sustenance value to the civilian population or to the adverse party, whatever the motive whether in order to starve out civilians, to cause them to move away, or for any motive.[22]

Mr. Church infers that in an industrialized society, the civilian population is highly dependent on centralized infrastructure systems such as water treatment facilities and power generation and distribution plants. Therefore, any attack on these systems will automatically have a direct impact on the civilian populace. It should be noted that Mr. Church footnoted the fact that the U.S. did not ratify the Protocol I Additional·[23]

In another article on IO, Mr. Church used the conflict in Kosovo as an example of how IO weapons were targeted at information infrastructure to affect government leadership and the general civilian populace.[24] Mr. Church gave his account and cited descriptions from "senior U.S. Air Force Officials" of how NATO used the full spectrum of IO activities including graphite bombs, covert system intrusions ("hacking"), an extensive psychological campaign, and hacking into insignificant web sites to affect the civilian population and to put pressure on the Yugoslavian government.[25] This action, he contends, raises significant international relations issues such as questions of sovereignty and the role of multinational organizations in the application of non-lethal technology weapons such as IO.

There is another unlikely promoter of a ban on IO attacks against information infrastructure targets. The Russian government, in 1998, requested that the United Nations establish a working group to study the development of a treaty for the use of IO.[26] While the Russian's motives in this initiative would appear to be suspect, there are others that recognize the new dimensions that modern IO could bring to the specter of war and have concerns about its indiscriminate use. Ms. Christine MacNulty, Chief Operating Officer of Applied Futures, Inc., sees a conflicting value system among those Americans that would view Information Warfare (IW) as simply an extension of conventional warfare and others who would view IW as "sneaky" and even un-American.[27] In mediating this situation, Ms. MacNulty states:

> Because of these conflicting views, we need to develop doctrine and policy that cover the ways in which information warfare can be employed and offer some guidance about the circumstances in which it should not be used. We need to do some clear thinking on these issues now. In time of war, commanders in the field are presented with sufficient ambiguity by the nature of the battlefield, itself. They need clear understanding about the employment of the information warfare weapons available to them so that (even if CNN is looking over their shoulders) their mission objectives can be their guiding principles.[28]

Ms. MacNulty makes a compelling case for the use of peacetime to debate the relevant issues and to develop an IO use policy that can be given to the military commander in the field before he has to engage the enemy. The U.S. soldier need not be distracted from his mission by having to consider the moral and ethical value issues involved in his directed use of IO. This sentiment is further resounded from the military itself. In a recent speech[29], Vice Admiral Herbert A. Browne, Deputy Commander in Chief of U.S. Space Command, stated that the rules of engagement for the captain of a U.S. frigate are currently sufficient that he could use a 5-inch gun to eliminate a maritime threat, possibly killing the crew. However, to use available IO tools to accomplish the same objective without the loss of life, the captain would have to get permission from the president. Admiral Browne went on to make three specific points:

> ...The U.S. needs rules of engagement that place tactical decisions on the use of information warfare assets in the hands of the tactical commanders.
>
> ...Similar rules for operational decisions – such as using information warfare tools to disable an air defense network – should be in the hands of theater, task force, or similar higher-level commanders.
>
> ...Rules of engagement for strategic decisions – attacking a nation's power grid or telecommunications network – should be in the hands of the national command authority.[30]

As previously stated, it would appear that most of the issues facing the U.S. on the use of IO during wartime, would be narrowed down to ethical ones, based in our national values. During peacetime, however, this entire matter gets much more complicated. There are a myriad of issues involving legalities, treaties, sovereignty, and acts of war that come into play. As the remaining super power and one of the world's largest users of high technology systems throughout its military, government and civilian infrastructure, the U.S. would face far greater potential consequences as a result of an IO attack. In layman's terms, the U.S. has more to loose. The U.S. has to consider carefully the impact of existing and proposed laws and treaties that may be entered into with other nations in respect to controlling or restricting IO activities.

During peacetime, the majority of the U.S. IO efforts are defensive in nature. They involve the protection of U.S. information infrastructure assets while actively gathering intelligence on possible and pending threats. These activities are collectively referred to as Information Assurance (IA):

> Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.[31]

Because the U.S. has a large stake in this matter, it has an obligation to protect its citizenry and its information resources by conducting a deliberate and aggressive IA program. The nature of the conduct of this program is where the laws, values and interests of the U.S.

versus those of other foreign states can come into conflict. In protecting its information and information systems, the U.S. is committed to going after those that attempt to gain unauthorized access into its computer-based systems (hackers). Domestically, the FBI, using existing U.S. laws would locate the perpetrator(s), confiscate their systems and prosecute them to the full extent of the law. However, when the attack comes from outside of the U.S., that effort takes on new dimensions.

One of the first problems the U.S. has is locating the attacker. Computer, network and switching technologies allow a hacker to enter the Internet or some subnet and traverse several other systems and networks before entering his target destination – effectively masking his point of origin. Even if located, it is not a given that the perpetrator will be brought to justice. At this point, there is the recognition that International law provides no right that entitles victim states to demand extradition.[32] In fact, the U.S. must satisfy four main criteria before achieving the extradition of a suspected cyber criminal.[33] First, there must be an existing extradition treaty between the two subject countries. Second, the requesting country must have laws that give its courts jurisdiction over foreign individuals who commit the specific crime alleged. Third, the "double criminality" requirement must be satisfied whereby, both treaty nations have domestic laws that proscribe the alleged conduct. Finally, there is no requirement to extradite where the act is a "political offense."

A recent study found that many nations have no laws to deal specifically with cyber crimes and other existing laws do little to deter crime in cyberspace.[34] The study involved fifty-two nations ranging from the U.S. to Albania. Recently, Representatives James Saxon, R-NJ. And Chambliss, R-GA, introduced legislation that calls on the U.S. government to develop a new legal framework to prosecute hackers and other Internet criminals.[35] The United Kingdom recently enacted The Terrorism Act 2000,[36] which broadened the definition of terrorists organizations to include those who plan violent protests in the UK (even if the protest takes place abroad). The Act was further expanded to cover cyber crimes and hackers, who have been written into the definition of a terrorist.

While criminal intent may cover one aspect of an attack, terrorism is another. So now we have the issue of locating the attacker, getting the resident country to concur that a crime has been committed and further determining if the individual is working alone, is representing an identifiable organization or is, in fact, an agent of that or another state. In dealing with conventional terrorism, the U.S. has demonstrated the willingness to act unilaterally in pursuing or retaliating against terrorist attacks. This has sometimes involved violating the sovereignty of another state. The 1988 air attack on Libya and the 2000 Tomahawk Land Attack Missile

(TLAM) attack against terrorist bases in Afghanistan are recent examples of this resolve. However, the evasive nature of technology shields the individuals and nation-states guilty of cyber attacks and complicates the justification the U.S. would have to conduct retaliatory strikes.

In making a case against an attacker, the U.S. may run into conflict with its own OPSEC program. Prosecuting an attacker might require the U.S. to divulge the mechanism by which the detection was made. Preserving knowledge of this capability may be more important to the U.S. than prosecuting this one individual attacker. However, there are publicly known capabilities for accomplishing this task. The Defense Advanced Research Projects Agency (DARPA) contracted with SRI International for the development of EMERALD (Event Monitoring Enabling Response to Anomalous Live Disturbances).[37] EMERALD can be used at entry points and throughout networks to detect and report anomalous behavior, misuse or other incoming attacks.[38] The EMERALD Program Manager further stated that development is underway to achieve the capability to connect this system to another system that could provide an immediate "response" capability.[39]

This is another area where a significant legal question arises – When does an aggressive defensive program become offensive and essentially constitutes computer attack itself? As mentioned above, computer software tools are becoming sufficiently sophisticated that they can provide near instantaneous response to illegal entry attempts. The form of this response becomes critical. Even the most passive response would involve tracking the attacker back to his point of origin and retrieving identifying data about that originator. However, in accomplishing this task, the previously attacked site has now possibly violated the sovereign boundaries of another country. The inexpensive availability of the required technical capabilities would allow an individual to perpetrate illegal actions against the U.S. and still provide the hosting state "plausible deniability" of that individual having any association with the state.[40] Further, that state could then voice indignation that its border had been violated.

This situation becomes further exacerbated when the U.S. decides to take a more aggressive response to the attack. Under Article 51 of the U.N. Charter, nations have the inherent right to defend themselves from and respond to "armed attack." However, it becomes debatable whether an attack on a U.S. information system would constitute an armed attack and, thereby, merit a proportional response. The U.S. could effectively make the case that because of the embedded nature of information systems in our society, such an attack could cause financial loss, interruption of services and even the loss of lives. The destruction of the attacker's computer system, through electronic means, compared to his potential to cause damage is far less than proportional. Accordingly, the destruction of that system by physical means puts the U.S. in a much more tenuous position, in terms of justifying its actions.

In defending its information systems during peacetime and in preparing to engage in wartime IO, the U.S. must conduct an aggressive intelligence-gathering program as part of its overall IO program. This is probably the most legally and socially contentious aspect of IO. In relations to the strategic arms limitations and reduction treaties, Dr. Dan Kuehl states that the ability to gather intelligence electronically has not only been understood and accepted but it has been enshrined in ethical correctness, in relations to the arms control lexicon, as "national technical means," a crucial part of the verification process.[41] However, in the past, the electronics involved were satellite systems and reconnaissance aircraft. Now that computer technology has become the available intelligence gathering means, the acceptability of this practice has been questioned. Now, using computer technologies, nations conducting intelligence gathering can "passively penetrate" and probe adversary systems.[42] As long as this probing is "passive" (Does not involve any manipulation or destruction of the probed system), does it constitute an attack of that adversary's system?

There is currently substantial concern among some U.S. citizens about the National Security Agency's ability to electronically gather intelligence and data; potentially about them. There are numerous websites dedicated to bringing attention to the ECHELON system.[43] This system has the ability to gather radio waves (satellite, microwave, UHF and VHF), filter recorded voice and data through computer programs and extract relevant security information. Organizations such as the American Civil Liberties Union (ACLU) worry that the NSA could go beyond national security and conduct routine surveillance of American citizens with this technology.

The Center for Democracy operates a website (www.cdt.org) where it provides a variety of information on issues relating to government invasion of privacy on its citizens. Included in that information is a chart that shows "Current Legal Standards for Access to Papers, Records and Communications." This chart breaks down various personal records and delineates the legal basis by which the government can or cannot access them. This site and others, such as those mentioned above, indicate the level of skepticism, distrust and downright paranoia that exist among people about the U.S. government's intelligence programs.

CONCLUSIONS.

Technology has burst onto the scene and it has blurred the lines of distinction and separation between many aspects of our global community. Information systems, especially the Internet, have given us the ability to be interconnected on a global basis. Companies operate different facets of their business in different countries on a seamless basis. These features of technology have been a tremendous benefit. However, when military issues, national sovereignty and security, and criminal activity and prosecution are considered, these same information systems and capabilities have created an intense amount of "battlefield fog." When used for negative purposes, these same systems have given birth to a new set of problems.

The interconnected and unbounded worldwide range of the Internet has also facilitated the emergence of the individual that takes pleasure in the unauthorized penetration of information networks and systems – the hacker. When plying his trade for fun, as an annoyance to others, or for financial gain, this individual is a criminal. When this same individual represents a larger group or organization and seeks to make a point for some political or other cause, especially across territorial borders, he is a terrorist. Further, when is the country from which he is operating a party to his act, especially when this nation is not aggressively aiding in his capture and prosecution?

There has been a collective recognition of the gap that has been created between information systems and IO programs and the laws that govern their use and operation. The U.S. Congress, the U.S. military and other nations, such as the United Kingdom (UK) have undertaken efforts to deal with legal guidelines that have not kept pace with the technology that they should govern. Previously discussed figures indicated that there are a large number of countries that have no laws at all to deal with cyber crimes. This problem becomes further acerbated when we consider the difficulty in achieving commonality between the laws of the different nations of the world. Different cultural, religious, moral and ethical values are thrown into the mix that significantly complicates the issue. The stringent laws of a victimized nation are nearly useless unless the offender's host nation has similar laws.

Domestically, the privacy and search and seizure laws of the U.S. significantly impair the ability of the government and military to actively pursue hackers, terrorists and spies. While I would not propose the mass abdication of individual rights, I feel that the elements of the U.S. government should work with the Department of Justice and the Congress to find ways to bring applicable laws into better synchronization with the high technology systems that exist now and into the future. For example, provisions could be made for authorities to obtain a search warrant to apprehend a cyber criminal while already in pursuit of that criminal. This pursuit would have begun after the offender had crossed a specified electronic barrier within an information system. The U.S. should further work with the UN, the World Court and other international organizations to establish reasonable laws that can be used to govern malicious, destructive and criminal acts involving information systems. Having said that, the U.S. should be prudent as not to enter into treaties that would hinder the effective conduct of its defensive IO programs. In the meantime, the U.S. must, unilaterally if necessary, vigorously pursue and prosecute cyber criminals and cyber terrorists if we are to maintain any degree of credible deterrence to cyber crime.

Just as with other intelligence programs, there are long-term elements of IO that must be cultivated well before they are needed. Intelligence gathering, system monitoring and probing of adversary systems are necessary to ascertain pending threats and to develop effective countermeasures. While steps are taken to close the gaps between applicable laws and current crimes, U.S. information systems should have built-in self-defensive measures that would prevent their destruction or long-term incapacitation.

During peacetime, the U.S. IO program must be sufficiently diligent as to defend our national information and information infrastructure from attack and to prepare us to effectively engage any enemy during wartime. The U.S., as the largest user of technology in the world, has many more information and information systems resources to protect and faces much more significant consequences in the event of an IO attack. It cannot afford to be meek in the measures that it takes to protect those resources.

When dealing with the offensive application of IO, the question boils down to when the U.S. would employ it and against what target. The nuclear arsenal of the U.S. is a necessary part of our deterrence against hostile forces. The destructive capability of these resources is enormous. However, they are maintained and controlled by a cadre of highly trained, professional members of the U.S. military. Their use, if required, is only authorized after executing an extensive authorization process that ends with the national command authority - the President. Even with this capability, the U.S. is committed to never initiating a first strike.

Our operation of an IO program must be (and is) carried out with an equal amount of diligence. During wartime, the choice of targets to be engaged by IO will be no less selective than those engaged with kinetic weapons. Consideration for collateral damage and the possible impact on noncombatants is, again, an associated component of the engagement process. The relative ease with which IO can be conducted should not be a primary determining factor in its use. The process of target identification and weapon selection should be based sound expert military principles and on the moral code by which the U.S. guides itself.

As one referenced author recommended, peacetime should be used to debate some of the relevant issues of IO such as those facilities and activities that should be permanently off of any target list. Hospitals, schools and financial institutions are facilities that are strictly civilian in nature and are critical to any post-hostilities society. Also, societal debate on the military use of IO gives the entire populace ownership in the consequences of such actions. In the case of the Viet Nam war, the ugliness of conducting war was left upon the soldier who actually had to do the fighting. We should address questions such as, "Does our probing of other systems make us hackers of another name?"

The U.S. must conduct its IO programs with equal control, oversight and prudence as to demonstrate the same high moral and ethical values under which we profess to live. Information and intelligence gathered using IO resources for the sake of national security should be a controlled resource. U.S. and global citizens of the world should not live in fear that the national security assets of the U.S. are engaged in recreational surveillance activities. The IO assets and capabilities of the U.S. should be as transparent as possible, without compromising security, to assure the American populace of its integrity and to deter would-be threats.

Total Word Count: 5,829 words

ENDNOTES

[1] General Accounting Office, Information Security: Opportunities for Improved OMB Oversight of Agency Practices (Chapter Report, 09/24/96, GAO/AIMD-96-110), (Washington, DC.:U.S. General Accounting Office, September 1996)

[2] John L. Woodward, Jr., Information Assurance through Defense in Depth, Directive from the Director for Command, Control, Communications and Computer Systems (J6), Joint Chiefs of Staff. (Washington, DC.: U.S. Department of Defense)

[3] Alan D. Campen; Douglas H. Dearth; and R. Thomas Goodden, eds. Cyberwar: Security, Strategy and Conflict in the information Age. (Fairfax: AFCEA International Press, 1996)

[4] "President's Commission on Critical Infrastructure Protection", July 1996; available from <http://www.ciao.gov/PCCIP/PCCIP_index.html>. Internet. Accessed 19 September 2000.

[5] White Paper, The Clinton Administration's policy on Critical Infrastructure Protection: Presidential Decision Directive 63, 28 July 1998; available from http://www.ciao.gov/PCCIP/report_index.html. Internet. Accessed 19 September 2000.

[6] William J. Clinton, A National Security Strategy for a New Century (Washington, D.C.: The White House, December 1999), 17.

[7] Secretary of Defense William Cohen, "Information Operations Condition (INFOCON)", Memorandum for the Secretaries of the Military Departments, Washington, D.C. , 10 March 1999, 1.

[8] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Publication 3-13, (Washington, D.C.: U.S. Joint Chiefs of Staff, 9 October, 1998), vii.

[9] Ibid., II-3

[10] Ibid., viii

[11] Ibid.

[12] Ibid., II-3

[13] Ibid., II-5

[14] As of this writing, the J39 staff structure is under review. Therefore further elaboration on staff functions will not be pursued.

[15] Ibid., IV-2

[16] Ibid., IV-3

[17] Ibid. (Note: The governing doctrine and the responsibility for and location of the IO Cell are currently under review.)

[18] Dan Kuehl, "The Ethics of Information Warfare and Statecraft," ; Available from http://www.infowar.com; Internet; accessed 15 January 2001.

[19] John Arquilla, "Ethics and Information Warfare," in The Changing Role of Information in Warfare, ed. Khalilzad, Aalmay and John White (Santa Monica: RAND, 1999), 383

[20] William Church, "Information Operations Violates Protocol I," 9 April 1999, available from http://www.infowar.com ; Internet; accessed 15 January 2001.

[21] Ibid.

[22] Ibid.

[23] Ibid.

[24] William Church, "Kosovo and the Future of Information Operations," 20 May 1999; available from www.infowar.com . Internet; Accessed 15 January 2001.

[25] Ibid.

[26] Ibid.

[27] Christine A. R. MacNulty, "Changing Values and Their Implications for the Ethics of Information Warfare," 31 July 1996; available from www.infowar.com. Internet; Accessed 15 January 2001.

[28] Ibid.

[29] "U.S. Forces Need Rules of Engagement for Cyberwar, Admiral Says," Aerospace Daily (10 July 2000).

[30] Ibid.

[31] Joint Publication 3-13. GL-7

[32] Michael J. Robbat, "Whether and How International Law Can Deal With the Use of IW by Nation-States and Terrorist Groups," Law Review, Boston University Journal of Science and Technology Law, Spring 2000 (Boston, MA: Boston University Press)

[33] Ibid.

[34] Jim Wolf, Study: Most Nations' Laws Lag on Cyber Crime," Reuters, 7 December 2000.

[35] Robert MacMillan, "Reps. Saxton, Chambliss Intro Cyber-Terrorism Measure," Newsbytes, February 9, 2001.

[36] Kieren McCarthy, "Hackers are Terrorists, Says UK Law," The Register, February 20, 2001.

[37] Jim Garamone, "DARPA's EMERALD Proves Worth In Cyberdefense," American Forces Press Service, 15 August 2000.

[38] Ibid.

[39] Ibid.

[40] Lawrence T. Greenberg, Seymour E. Goodman and Kevin J. Soo Hoo, "Responding to Information Warfare Attacks: International Legal Issues and Approaches," in Information Warfare and International Law (Washington, D.C.: National Defense University Press)

[41] Kuehl.

[42] Ibid.

[43] ECHELON is a worldwide satellite-based signal intelligence gathering network operated by "UKUSA". UKUSA is a consortium of nations that grew out of 1948 agreement between the United Kingdom and the USA to share intelligence capabilities. The network currently has participating sites from Canada (CSE – Communications Security Establishment), United Kingdom (GCHQ – Government Communications HQ), New Zealand (GCSB – Government Communications Security Bureau) and the United States' National Security Agency.

BIBLIOGRAPHY

"President's Commission on Critical Infrastructure Protection", July 1996; available from <http://www.ciao.gov/PCCIP/PCCIP_index.html>. Internet. Accessed 19 September 2000.

"U.S. Forces Need Rules of Engagement for Cyberwar, Admiral Says," Aerospace Daily (10 July 2000).

Arquilla, John, "Ethics and Information Warfare," in The Changing Role of Information in Warfare, ed. Khalilzad, Aalmay and John White (Santa Monica: RAND, 1999)

Campen, Allen D.; Dearth, Douglas H.; and Goodden, R. Thomas, Eds. Cyberwar: Security, Strategy and Conflict in the information Age. Fairfax: AFCEA International Press, 1996.

Church, William, "Information Operations Violates Protocol I," 9 April 1999, available from http://www.infowar.com ; Internet; accessed 15 January 2001.

Church, William, "Kosovo and the Future of Information Operations," 20 May 1999; available from www.infowar.com ; Internet; Accessed 15 January 2001.

Clinton, William J., A National Security Strategy for a New Century Washington, D.C.: The White House, December 1999.

Cohen, William, Secretary of Defense, "Information Operations Condition (INFOCON)", Memorandum for the Secretaries of the Military Departments, Washington, D.C., 10 March 1999.

Garamone, Jim, "DARPA's EMERALD Proves Worth In Cyberdefense," American Forces Press Service, 15 August 2000.

Greenberg, Lawrence T., Goodman, Seymour E. and Soo Hoo, Kevin J., "Responding to Information Warfare Attacks: International Legal Issues and Approaches," in Information Warfare and International Law. Washington, D.C.: National Defense University Press.

Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Publication 3-13, Washington, D.C.: U.S. Joint Chiefs of Staff, 9 October, 1998.

Kuehl, Dan, "The Ethics of Information Warfare and Statecraft,"; Available from http://www.infowar.com; Internet; accessed 15 January 2001.

MacMillan, Robert, "Reps. Saxton, Chambliss Intro Cyber-Terrorism Measure," Newsbytes, February 9, 2001.

MacNulty, Christine A. R., "Changing Values and Their Implications for the Ethics of Information Warfare," 31 July 1996; available from www.infowar.com; Internet; Accessed 15 January 2001.

McCarthy, Kieren, "Hackers are Terrorists, Says UK Law," The Register, February 20, 2001.

Robbat, Michael J., "Whether and How International Law Can Deal With the Use of IW by Nation-States and Terrorist Groups," Law Review, Boston University Journal of Science and Technology Law, Spring 2000. Boston, MA: Boston University Press.

U.S. General Accounting Office, Information Security: Opportunities for Improved OMB Oversight of Agency Practices (Chapter Report, 09/24/96, GAO/AIMD-96-110). Washington, D.C.: U.S. General Accounting Office, September 1996.

White Paper, The Clinton Administration's policy on Critical Infrastructure Protection: Presidential Decision Directive 63, 28 July 1998; available from http://www.ciao.gov/PCCIP/report_index.html. Internet. Accessed 19 September 2000.

Wolf, Jim, Study: Most Nations' Laws Lag on Cyber Crime," Reuters, 7 December 2000.

Woodward, John L. Jr., Information Assurance through Defense in Depth, Directive from the Director for Command, Control, Communications and Computer Systems (J6), Joint Chiefs of Staff. Washington, DC.: U.S. Department of Defense, 1997.